CLAIMS:

1. A multi-protocol, videoconferencing interface device, comprising:

at least three encryption devices, each encryption device configured to encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol;

a secure interface connecting the at least three encryption devices, and configured to relay video and audio traffic between the at least three encryption devices during a common videoconferencing event;

a videoconferencing data buffer connected to the secure interface and configured to buffer traffic relayed between the at least three encryption devices during the common videoconferencing event; and

a videoconferencing management data archive connected to the secure interface and configured to hold the link-unique encryption keys, wherein

said multi-protocol, videoconferencing interface device is one of a gateway device and a multi-point control unit (MCU) device.

2. The multi-protocol, videoconferencing interface device of Claim 1, wherein the videoconferencing management data archive is further configured to store at least one of:

a management information;

a session history;

a diagnostic information; and

a session scheduling and billing information.

3. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface comprises:

a key management device.

4. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface comprises:

an encryption device programming device configured to enable one of local and remote encryption programming.

5. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface comprises:

a videoconference scheduling device.

6. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface comprises:

a key management and synchronization device.

7. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface comprises:

an encryption protocol management and synchronization device.

8. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface comprises:

a billing and account management device.

9. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface comprises:

a videoconferencing diagnostics device.

10. The multi-protocol, videoconferencing interface device of Claim 1, wherein the secure interface engine comprises:

a communications protocol translator configured to translate between at least two link-unique communications protocols.

11. The multi-protocol, videoconferencing interface device of Claim 10, wherein

a first of the at least two link-unique communications protocols comprises one of H.320, H.323, H.324, and T.120; and

a second of the of the at least two link-unique communications protocols comprises another of H.320, H.323, H.324, and T.120

12. The multi-protocol, videoconferencing interface device of Claim 1, wherein each of the link-unique encryption protocols comprises one of:

a manually provided encryption protocol;

a DES protocol;
a triple-DES protocol;
an AES protocol; and
an IDEA protocol.

13. The multi-protocol, videoconferencing interface device of Claim 1, wherein at least one of the at least three encryption devices is configured to exchange keys via a key encryption protocol comprising one of:

an automatic key exchange protocol; and
a manual key exchange protocol.

14. The multi-protocol, videoconferencing interface device of Claim 13, wherein the automatic key exchange protocol comprises one of:

a Diffie-Helman protocol; and
an RSA protocol.

15. A multi-protocol, videoconferencing interface device, comprising:

at least four encryption devices, each encryption device configured to encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol;

a first and a second secure interface engine connected to each other, connecting the at least four encryption devices, and configured to relay video and audio traffic between the at least four encryption devices during a common videoconferencing event;

a first and a second videoconferencing data buffer connected to the first and second secure interface engines, respectively, and configured to buffer traffic relayed between the at least four encryption devices during the common videoconferencing event; and

a first and a second videoconferencing management data archive connected to the first and the second secure interface engines, respectively, and configured to hold respective encryption keys, wherein

said multi-protocol, videoconferencing interface device is one of a gateway device and a multi-point control unit (MCU) device.

16. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second videoconferencing management data archives is further configured to store at least one of:

a management information;

a session history;

a diagnostic information; and

a session scheduling and billing information.

17. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second secure interface engines comprises:

a key management device.

18. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second secure interface engines comprises:

an encryption device programming device configured to enable one of local and remote encryption programming.

19. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second secure interface engine comprises:

a videoconference scheduling device.

20. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second secure interface engines comprises:

a key management and synchronization device.

21. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second secure interface engines comprises:

an encryption protocol management and synchronization device.

22. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and secure interface engines comprises:

a billing and account management device.

23. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second secure interface engines comprises:

a videoconferencing diagnostics device.

24. The multi-protocol, videoconferencing interface device of Claim 15, wherein one of the first and second secure interface engines comprises:

a communications protocol translator configured to translate between at least two link-unique communications protocols.

25. The multi-protocol, videoconferencing interface device of Claim 24, wherein

a first of the at least two link-unique communications protocols comprises one of H.320, H.323, H.324, and T.120; and

a second of the of the at least two link-unique communications protocols comprises another of H.320, H.323, H.324, and T.120

26. The multi-protocol, videoconferencing interface device of Claim 15, wherein each of the link-unique encryption protocols comprises one of:

a manually provided encryption protocol;

a DES protocol;

a triple-DES protocol;

an AES protocol; and

an IDEA protocol.

27. The multi-protocol, videoconferencing interface device of Claim 15, wherein at least one of the at least four encryption devices is configured to exchange keys via a key encryption protocol comprising one of:

an automatic key exchange protocol; and

a manual key exchange protocol.

28. The multi-protocol, videoconferencing interface device of Claim 27, wherein the automatic key exchange protocol comprises one of:

a Diffie-Helman protocol; and

an RSA protocol.

29. A multi-protocol, videoconferencing interface system, comprising:

a first, second, and third videoconferencing node, each videoconferencing node including a node encryption device; and

a multi-protocol, videoconferencing interface device connected to the first, second, and third videoconferencing nodes, and including

three interface encryption devices, each interface encryption device configured to encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol, the three interface encryption devices connected to a corresponding node encryption device ;

a secure interface connecting the three encryption devices, and configured to relay video and audio traffic between the three encryption devices during a common videoconferencing event;

a videoconferencing data buffer connected to the secure interface and configured to buffer traffic relayed between the three encryption devices during the common videoconferencing event; and

a videoconferencing management data archive connected to the secure interface and configured to hold the link-unique encryption keys wherein

said multi-protocol, videoconferencing interface device is one of a gateway device and a multi-point control unit (MCU) device.

30. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface comprises:

a key management device.

31. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface comprises:

an encryption device programming device configured to enable one of local and remote encryption programming.

32. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface comprises:

a videoconference scheduling device.

33. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface comprises:

a key management and synchronization device.

34. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface comprises:

an encryption protocol management and synchronization device.

35. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface comprises:

a billing and account management device.

36. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface comprises:

a videoconferencing diagnostics device.

37. The multi-protocol, videoconferencing interface system of Claim 29, wherein the secure interface engine comprises:

a communications protocol translator configured to translate between at least two link-unique communications protocols.

38. A multi-protocol, videoconferencing interface system, comprising:

a first, second, third, and fourth videoconferencing node, each videoconferencing node including a node encryption device; and

a multi-protocol, videoconferencing interface device connected to the first, second, third, and fourth videoconferencing nodes, and including

four encryption devices, each encryption device configured to encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol, the four interface encryption devices connected to a corresponding node encryption device;

a first and a second secure interface engine connected to each other, connecting the four encryption devices, and configured to relay video and audio traffic between the four encryption devices during a common videoconferencing event;

a first and a second videoconferencing data buffer connected to the first and second secure interface engines, respectively, and configured to buffer traffic relayed between the four encryption devices during the common videoconferencing event; and

a first and a second videoconferencing management data archive connected to the first and the second secure interface engines, respectively, and configured to hold respective encryption keys wherein

said multi-protocol, videoconferencing interface device is one of a gateway device and a multi-point control unit (MCU) device.

39. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

a key management device.

40. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

an encryption device programming device configured to enable one of local and remote encryption programming.

41. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

a videoconference scheduling device.

42. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

a key management and synchronization device.

43. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

an encryption protocol management and synchronization device.

44. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

a billing and account management device.

45. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

a videoconferencing diagnostics device.

46. The multi-protocol, videoconferencing interface system of Claim 38, wherein one of the first and second secure interfaces comprises:

a communications protocol translator configured to translate between at least two link-unique communications protocols.

47. A method for secure, multi-protocol videoconferencing, comprising:

receiving at an interface device a first set of encrypted video data from a first terminal over a first data communications link including a first communications protocol;

decrypting the first set of video data at the interface device; and

re-encrypting and relaying the first set of data from the interface device to

a second terminal over a second communication link having a second communications protocol, the second communications protocol different from the first communications protocol, and

a third terminal over a third communication link having a third communications protocol.

48. The method of Claim 47, wherein the third communications protocol comprises:

a communications protocol different from both the first and second communications protocols.

49. The method of Claim 47, wherein the third communications protocol comprises:

a communications protocol the same as one of the first and second communications protocols.

50. The method of Claim 47, wherein

the step of decrypting the first set of video data comprises decrypting with a first encryption key and a first encryption protocol, and

the step of re-encrypting and sending the first set of video data to the second terminal comprises encrypting the first set of video data with a second encryption key and a second encryption protocol, the second encryption key different from the first encryption key and the second encryption protocol different from the first encryption protocol.

51. The method of Claim 50, wherein the step of re-encrypting and sending the first set of video data to the third terminal further comprises:

encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols.

52. The method of Claim 50, wherein the step of re-encrypting and sending the first set of video data to the third terminal further comprises:

encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols.

53. The method of Claim 50, wherein the step of re-encrypting and sending the first set of video data to the third terminal further comprises:

encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being the same as one of the first and second encryption keys and the third encryption protocol being the same as a corresponding one of the first and second encryption protocols.

54. The method of Claim 47, wherein

the step of decrypting the first set of video data comprises decrypting with a first encryption key and a first encryption protocol, and

the step of re-encrypting and sending the first set of video data to the second terminal comprises encrypting with a second encryption key and a second encryption protocol, the second encryption key different from the first encryption key and the second encryption protocol the same as the first encryption protocol.

55. The method of Claim 54, wherein the step of re-encrypting and sending the first set of video data to the third terminal further comprises:

encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols.

56. The method of Claim 54, wherein the step of re-encrypting and sending the first set of video data to the third terminal further comprises:

encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols.

57. The method of Claim 47, further comprising:

receiving at the interface device a second set of encrypted video data from the second terminal over the second data communication link;

decrypting the second set of video data at the interface device with a second key and a second encryption protocol; and

re-encrypting and relaying the second set of data from the interface device to the first terminal and the third terminal via the first and third communications links, respectively.

58. The method of Claim 57, wherein the third communications protocol comprises:

a communications protocol different from both the first and second communications protocols

59. The method of Claim 57, wherein the third communications protocol comprises:

a communications protocol the same as one of the first and second communications protocols

60. The method of Claim 57, wherein

the step of decrypting the second set of video data comprises decrypting with a second encryption key and a second encryption protocol, and

the step of re-encrypting and sending the second set of video data to the first terminal comprises encrypting with the first encryption key and the first encryption protocol, the second encryption key different from the first encryption key and the second encryption protocol different from the first encryption protocol.

61. The method of Claim 60, wherein the step of re-encrypting and sending the second set of video data to the third terminal further comprises:

encrypting with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols.

62. The method of Claim 60, wherein the step of re-encrypting and sending the second set of video data to the third terminal further comprises:

encrypting with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols.

63. The method of Claim 60, wherein the step of re-encrypting and sending the second set of video data to the third terminal further comprises:

encrypting with a third encryption key and a third encryption protocol, the third encryption key being the same as one of the first and second encryption keys and the third encryption protocol being the same as a corresponding one of the first and second encryption protocols.

64. The method of Claim 57, wherein

the step of re-encrypting and sending the second set of video data to the first terminal comprises encrypting with a first encryption key and a first encryption protocol, the second encryption key different from the first encryption key and the second encryption protocol the same as the first encryption protocol.

65. The method of Claim 64, wherein the step of re-encrypting and sending the second set of video data to the third terminal further comprises:

encrypting with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols.

66. The method of Claim 64, wherein the step of re-encrypting and sending the second set of video data to the third terminal further comprises:

encrypting with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols.

67. The method of Claim 57, further comprising:

receiving at the interface device a third set of encrypted video data from the third terminal over the third data communication link;

decrypting the third set of video data at the interface device with a third encryption key and a third encryption protocol; and

re-encrypting and relaying the third set of data from the interface device to the first and second terminals over the first and second communication links, respectively.

68. The method of Claim 67, wherein the third communication protocol comprises:

a communications protocol different from the first and second communications protocols.

69. The method of Claim 67, wherein the third communication protocol comprises:

a communications protocol the same as one of the first and second communications protocols.

70. The method of Claim 67, wherein

the step of re-encrypting and sending the third set of video data to the first terminal comprises encrypting with a first encryption key and a first encryption protocol,

the step of re-encrypting and sending the third set of video data to the second terminal comprises encrypting with a second encryption key and a second encryption protocol, the second encryption key different from the first encryption key and the second encryption protocol different from the first encryption protocol.

71. The method of Claim 70, wherein the step of decrypting with a third encryption key and a third encryption protocol comprises:

decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol different from the first and second encryption protocols.

72. The method of Claim 70, wherein the step of decrypting with a third encryption key and a third encryption protocol comprises:

decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol the same as one of the first and second encryption protocols.

73. The method of Claim 70, wherein the step of decrypting with a third encryption key and a third encryption protocol comprises:

decrypting with a third encryption key the same as one of the first and second encryption keys and a third encryption protocol the same as a corresponding one of the first and second encryption protocols.

74. The method of Claim 67, wherein

the step of re-encrypting and sending the third set of video data to the first terminal comprises encrypting with a first encryption key and a first encryption protocol, and

the step of re-encrypting and sending the third set of video data to the second terminal comprises encrypting with a second encryption key different from the first encryption key and a second encryption protocol the same as the first encryption protocol.

75. The method of Claim 74, wherein the step of decrypting with a third encryption key and a third encryption protocol comprises:

decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol different from the first and second encryption protocols.

76. The method of Claim 74, wherein the step of decrypting with a third encryption key and a third encryption protocol comprises:

decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol the same as one of the first and second encryption protocols.

77. A system for secure, multi-protocol videoconferencing, comprising:

means for receiving at an interface device a first set of encrypted video data from a first terminal over a first data communications link including a first communications protocol;

means for decrypting the first set of video data at the interface device; and

means for re-encrypting and relaying the first set of data from the interface device to

a second terminal over a second communication link having a second communications protocol, the second communications protocol different from the first communications protocol, and

a third terminal over a third communication link having a third communications protocol.

78. A computer program product configured to store instructions corresponding to any one of the methods of Claims 47-76.